

AMENDMENTS TO THE CLAIMS

Please amend the claims of the present application as set forth below. This listing of claims will replace all prior versions and listings of claims in the application.

Claims 1, 4-19, 21-27, 29-31, and 33-42 were pending at the time of the Final Office Action.

Claims 1, 4-19, 21-27, 29-30, and 35-42 are currently pending as a result of this communication.

Claims 1, 4, 6, 8, 19, 26, and 35 are currently amended.

Claims 2, 3, 20, 28, and 31-34 are cancelled without prejudice or disclaimer.

Listing of Claims

1. (Currently amended) A system comprising:

a pluggable security policy enforcement module configured to be replaceable in the system and to provide different granularities of control for a business logic in the system, wherein the business logic processes requests submitted to the system, wherein the business logic contains problem-solving logic that produces solutions for a particular problem domain,

wherein the pluggable security policy enforcement module is configured to determine, for a particular granularity of control, whether to permit an operation, requested by a user based at least in part on a permission assigned to the user, and wherein the business logic employs interaction-based definitions in which a component which performs the operation is defined by a series of request-response interaction definitions that can be satisfied to perform the operation.

1 and wherein the different granularities of control comprise a plurality of sets of
2 rules that can be replaced with each other without altering the business logic.

3
4 2. (Cancelled).

5
6 3. (Cancelled).

7
8 4. (Currently amended) A system comprising:

9 a pluggable security policy enforcement module configured to be replaceable in
10 the system and to provide different granularities of control for a business logic in the
11 system, wherein the business logic processes requests submitted to the system, wherein
12 the business logic contains problem-solving logic that produces solutions for a particular
13 problem domain, and wherein the business logic employs interaction-based definitions in
14 which a component which performs an operation associated with an individual request is
15 defined by a series of request-response interaction definitions that can be satisfied to
16 perform the operation,

17 wherein the pluggable security policy enforcement module includes a control
18 module configured to determine whether to permit an operation based at least in part on
19 accessing the business logic to identify one or more additional tests to perform, and
20 further configured to perform the one or more additional tests.

21
22 5. (Original) A system as recited in claim 4, wherein the control module is further
23 configured to return a result of the determining to the business logic.

24
25 6. (Currently amended) A system comprising:

1 a pluggable security policy enforcement module configured to be replaceable in
2 the system and to provide different granularities of control for a business logic in the
3 system, wherein the business logic processes requests submitted to the system, and
4 wherein the business logic employs interaction-based definitions in which a component
5 which performs an operation associated with an individual request is defined by a series
6 of request-response interaction definitions that can be satisfied to perform the operation,

7 wherein the different granularities of control comprise a plurality of sets of rules,
8 and wherein each set of rules includes a plurality of permission assignment objects,
9 wherein each of the permission assignment objects associates a user with a particular
10 role, wherein each particular role is associated with one or more permissions, and
11 wherein each of the one or more permissions identifies a particular operation and context
12 on which the operation is to be performed.

13
14 7. (Original) A system as recited in claim 6, wherein each of the permission
15 assignment objects further identifies whether the one or more permissions in the
16 particular role are granted to the user or denied to the user.

17
18 8. (Currently amended) One or more computer-readable media comprising
19 computer-executable instructions that, when executed, direct a processor to perform acts
20 including:

21 receiving a request to perform an operation;

22 checking whether to access a business logic in order to generate a result for the
23 requested operation, wherein the business logic contains problem-solving logic that
24 produces solutions for a particular problem domain, and wherein the business logic
25 employs interaction-based definitions in which a component which performs an operation

1 associated with the request is defined by a series of request-response interaction
2 definitions that can be satisfied to perform the operation;

3 obtaining, from the business logic, a set of zero or more additional tests to be
4 performed in order to generate the result;

5 performing each additional test in the set of tests if there is at least one test in the
6 set of tests;

7 checking a set of pluggable rules to determine the result of the requested
8 operation; and

9 returning, as the result, a failure indication if checking the business logic or
10 checking the set of pluggable rules indicates that the result is a failure, otherwise
11 returning, as the result, a success indication.

12
13 9. (Original) One or more computer-readable media as recited in claim 8, wherein
14 the receiving comprises receiving, from the business logic, the request to perform the
15 operation.

16
17 10. (Original) One or more computer-readable media as recited in claim 8,
18 wherein the receiving comprises receiving, as part of the request, an indication of a user,
19 and wherein the checking the set of pluggable rules comprises comparing an object
20 associated with the user to the rules in the set of pluggable rules and determining whether
21 the operation can be performed based at least in part on whether the user is permitted to
22 perform the operation.

23
24 11. (Original) One or more computer-readable media as recited in claim 8,
25 wherein the receiving comprises having one of a plurality of methods invoked.

1
2 12. (Original) One or more computer-readable media as recited in claim 8,
3 wherein the set of pluggable rules is a set of security rules defined using high-level
4 permission concepts.

5
6 13. (Original) One or more computer-readable media as recited in claim 12,
7 wherein the high-level permission concepts include an operation and a context, wherein
8 the operation allows identification of an operation to be performed and the context allows
9 identification of what the operation is to be performed on.

10
11 14. (Original) One or more computer-readable media as recited in claim 8,
12 wherein the computer-executable instructions are implemented as an object.

13
14 15. (Original) One or more computer-readable media as recited in claim 8,
15 wherein the computer-executable instructions further direct the processor to perform acts
16 including:

17 determining if at least one of the tests in the set of zero or more additional tests
18 would indicate a result of failure; and

19 returning, as the result, the failure indication without checking the set of
20 pluggable rules.

21
22 16. (Original) One or more computer-readable media as recited in claim 8,
23 wherein the set of pluggable rules can be replaced with another set of pluggable rules
24 without altering the business logic.

1 17. (Original) One or more computer-readable media as recited in claim 8,
2 wherein the set of pluggable rules includes a plurality of permission assignment objects,
3 wherein each of the permission assignment objects associates a user with a particular
4 role, wherein each particular role is associated with one or more permissions, and
5 wherein each of the one or more permissions identifies a particular operation and context
6 on which the operation is to be performed.

7
8 18. (Original) One or more computer-readable media as recited in claim 17,
9 wherein each of the permission assignment objects further identifies whether the one or
10 more permissions in the particular role are granted to the user or denied to the user.

11
12 19. (Currently amended) A method comprising:
13 providing high-level permission concepts for security rules;
14 allowing a set of security rules to be defined using the high-level permission
15 concepts, wherein the set of security rules allows permissions to be assigned to users of
16 an application; and
17 determining, based at least in part on a permission assigned to a user, whether to
18 permit an operation based on a request by the user,
19 wherein the determining further comprises determining whether to permit the
20 operation requested by the user based at least in part on accessing a business logic to
21 identify one or more additional tests to perform, and further comprising performing the
22 one or more additional tests, wherein the business logic contains problem-solving logic
23 that produces solutions for a particular problem domain, and wherein the business logic
24 employs interaction-based definitions in which a component which performs the
25

1 operation is defined by a series of request-response interaction definitions that can be
2 satisfied to perform the operation.

3
4 20. (Canceled).

5
6 21. (Previously presented) A method as recited in claim 19, further comprising
7 returning a result of the determining to the business logic.

8
9 22. (Original) A method as recited in claim 19, wherein the high-level permission
10 concepts include an operation and a context, wherein the operation allows identification
11 of an operation to be performed and the context allows identification of what the
12 operation is to be performed on.

13
14 23. (Original) A method as recited in claim 19, wherein the method is
15 implemented in an object having a plurality of interfaces for requesting a determination
16 as to whether to permit a plurality of operations including the operation requested by the
17 user.

18
19 24. (Original) A method as recited in claim 19, wherein the set of security rules
20 includes a plurality of permission assignment objects, wherein each of the permission
21 assignment objects associates a user with a particular role, wherein each particular role is
22 associated with one or more permissions, and wherein each of the one or more
23 permissions identifies a particular operation and context on which the operation is to be
24 performed.

1 25. (Original) A method as recited in claim 24, wherein each of the permission
2 assignment objects further identifies whether the one or more permissions in the
3 particular role are granted to the user or denied to the user.

4
5 26. (Currently amended) A method comprising:
6 receiving a request to perform an operation associated with business logic,
7 wherein the business logic contains problem-solving logic that produces solutions for a
8 particular problem domain, and wherein the business logic employs interaction-based
9 definitions in which a component which performs the operation is defined by a series of
10 request-response interaction definitions that can be satisfied to perform the operation;
11 accessing a set of low-level rules, wherein the low-level rules are defined in terms
12 of high-level concepts;
13 checking whether a user requesting to perform the operation is entitled to perform
14 the operation based at least in part on the set of low-level rules; and
15 returning an indication of whether the operation is allowed or not allowed,
16 wherein the set of low-level rules can be replaced with another set of low-level
17 rules without altering the business logic.

18
19 27. (Previously presented) A method as recited in claim 26, wherein the checking
20 further comprises checking whether the user is entitled to perform the operation based at
21 least in part on accessing the business logic to identify one or more additional tests to
22 perform, and further comprising performing the one or more additional tests.

23
24 28. (Canceled).
25

1 29. (Original) A method as recited in claim 27, further comprising returning the
2 indication to the business logic.

3
4 30. (Original) A method as recited in claim 26, wherein the low-level rules
5 include a plurality of permission assignment objects, wherein each of the permission
6 assignment objects associates a user with a particular role, wherein each particular role is
7 associated with one or more permissions, and wherein each of the one or more
8 permissions identifies a particular operation and context on which the operation is to be
9 performed

10
11 31. – 34. (Cancelled).

12
13 35. (Currently amended) An architecture comprising:

14 a plurality of resources;

15 a business logic layer to process, based at least in part on the plurality of
16 resources, requests received from a client, wherein the business logic layer contains
17 problem-solving logic that produces solutions for a particular problem domain, and
18 wherein the business logic employs interaction-based definitions in which a component
19 which performs an operation corresponding to an individual request is defined by a series
20 of request-response interaction definitions that can be satisfied to perform the operation;
21 and

22 a pluggable security policy enforcement module, separate from the business logic
23 layer, to enforce security restrictions on accessing information stored at the plurality of
24 resources.

1 36. (Original) An architecture as recited in claim 35, wherein the pluggable
2 security policy enforcement module defines high-level permission concepts for security
3 rules and further defines a set of security rules using the high-level permission concepts.
4

5 37. (Original) An architecture as recited in claim 36, wherein the high-level
6 permission concepts include an operation and a context, wherein the operation allows
7 identification of an operation to be performed and the context allows identification of
8 what the operation is to be performed on.
9

10 38. (Original) An architecture as recited in claim 35, wherein the pluggable
11 security policy enforcement module can be replaced with another pluggable security
12 policy enforcement module to enforce different security restrictions without altering the
13 business logic layer.
14

15 39. (Original) An architecture as recited in claim 35, wherein the pluggable
16 security policy enforcement module is configured to determine, based at least in part on a
17 permission assigned to a user and on one or more additional tests identified by accessing
18 the business logic layer, whether to permit an operation to access information at the
19 plurality of resources.
20

21 40. (Previously presented) A system as recited in claim 1, wherein the system is
22 configured as a multi-layer architecture, wherein the business logic is implemented as a
23 business logic layer of the multi-layer architecture.
24
25

1 41. (Previously presented) A system as recited in claim 1, wherein the pluggable
2 security policy enforcement module is configured to receive an input from the business
3 logic in the form of a user indication and an item indication.

4
5 42. (Previously presented) A system as recited in claim 1, wherein the pluggable
6 security policy module includes an interface that provides the following interface
7 functionality:

8 first functionality for testing whether an identified item can be approved by a
9 specified user;

10 second functionality for testing whether the identified item of a specified type can
11 be created by the specified user;

12 third functionality for testing whether the identified item can be deleted by the
13 specified user;

14 fourth functionality for testing whether the identified item can be modified by the
15 specified user; and

16 fifth functionality for testing whether the identified user can examine details of
17 the identified item.